THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic

November 6, 2008

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Federal Government has long recognized the importance of the delivery of national security and emergency preparedness (NS/EP) traffic regardless of the condition of and circumstances surrounding the communications networks. Over the past several decades, the President's National Security Telecommunications Advisory Committee (NSTAC) has provided guidance on how to prioritize NS/EP traffic in times of crisis. Specifically, the NSTAC's industry partners developed recommendations to the President regarding NS/EP communications traffic prioritization that prompted the Department of Homeland Security's (DHS) National Communications System (NCS) to create the Nation's current priority service programs—Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS). With these services, NS/EP users have a high probability of completing calls even during times of network stress.

Service providers have invested billions of dollars to both transform and augment their circuit-switched networks to incorporate the use of technologies based on Internet protocol (IP). As the core networks universally evolve from circuit-switched to packet-based service technologies, it is important for the Federal Government to consider the impact of this evolution on the delivery of NS/EP communications traffic.

Although the rapid growth of the Internet has led to exciting new services for customers, such as Voice over IP (VoIP), these technological advancements have also altered the NS/EP priority-services network environment. To address the need for the continued delivery of NS/EP traffic over packet-based networks, during the 2007 NSTAC Meeting, the Assistant to the President for Homeland Security and Counterterrorism requested that the NSTAC examine concerns regarding the risk, if any, to IP-based NS/EP communications traffic, including VoIP, during times of perceived abnormal conditions or network duress. Specifically, the White House requested that the NSTAC determine if network degradation or disruption could affect the receipt or delivery of NS/EP traffic and, if so, asked that the NSTAC provide recommendations to the President regarding measures to ensure the delivery of IP-based NS/EP traffic during times of network duress.

To conduct its analysis, the NSTAC examined how service providers transport IP-based traffic across their networks and how they shared data regarding their ability to manage traffic end-to-end. The NSTAC also examined how carriers and service providers offer managed services to meet the requirements of their enterprise customers, including some NS/EP authorized users. After completing its examination, the NSTAC found:

- The core networks are universally evolving from circuit-switched to packet-based service technologies. The network management principles employed by the carriers evolve as the technology of the networks advances, including the ability to manage traffic within and across IP-based network overlays.

- The growth of high-bandwidth applications has led to higher traffic levels and could affect NS/EP communications traffic. Service providers design and manage their

networks to avoid or minimize network congestion and to prevent and respond to network events.

- Enhanced services for NS/EP authorized users in a packet-based network environment must begin with traffic management within customer equipment, such as enterprise routers, servers, and terminal devices, prior to connecting to the service provider/transport portion of the network.

- The public Internet handles packet routing on a best-effort basis, meaning it will try its best to forward user traffic, but can provide no guarantees regarding loss rate, bandwidth, delay, and/or jitter.[1]

- Within a single network via a managed service offering, a service provider can offer performance/reliability assurances because it is able to monitor and manage services on an end-to-end basis. A customer can also enter into an agreement with multiple service providers to receive a specific quality of service (QoS) from the service providers for a managed service.

- The Federal Government uses managed services to meet its communications needs. NS/EP services could also be provisioned using managed services within the new IP-based environment.

- The Nation's NS/EP capabilities based on the public switched telephone network (PSTN) continue to support key leadership and first responders using GETS, WPS and TSP, but with the increasing consumer and commercial adoption of IP-based communications, its long-term viability is diminishing.

- The NCS is working with industry partners to establish IP-based priority services using an "industry requirements" model, which was previously successful in developing the GETS and WPS solutions. Continued funding for these NCS activities is essential to enable continued Government and industry collaboration and to ensure that advanced NS/EP services are there when needed.

- Global standards bodies are addressing NS/EP IP-based priority services delivery. The United States has an opportunity to influence the outcomes of these standards bodies by actively participating and leading the standards development process.

- The Federal Communications Commission (FCC) found that the provision of priority services offered to NS/EP authorized users was *prima facie* lawful under the *Communications Act of 1934.* These priority services support critical functions such as national security leadership, continuity of government, public health, and safety, maintenance of law and order, and disaster recovery during national security

[1] Jitter is defined as any disruption in packet transmission or delivery.

emergencies. This provision must maintain the authority to ensure that networks remain capable of providing priority communications for NS/EP authorized users in the future.

The NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, that the President should:

- In the short term, establish a policy that requires Federal departments and agencies to:
  - Ensure their enterprise networks are properly designed and engineered to handle high traffic volume;
  - Manage traffic through QoS programming in its routers to prioritize traffic, including NS/EP traffic; and
  - Expand the use of managed service agreements to provision NS/EP services within the new IP-based environment.

- In the long term, require that Federal departments and agencies remain actively involved in standards development of priority services on IP-based networks by supporting efforts to:
  - Provide adequate funding that will be used to develop timely solutions across all technology platforms; and
  - Commit appropriate resources to actively participate in and lead the global standards bodies' efforts to address NS/EP IP-based priority services.

- Petition the FCC for a declaratory ruling to confirm that network service providers may lawfully provide IP-based priority access services to NS/EP authorized users.

1.0 INTRODUCTION

1.1 Background

The Federal Government has long recognized the importance of optimizing the delivery of national security and emergency preparedness (NS/EP) traffic regardless of network conditions. Over the past several decades, the President's National Security Telecommunications Advisory Committee (NSTAC) has provided guidance to the President on how to prioritize of NS/EP traffic in times of crisis. As a result of that guidance, the Federal Government now operates three priority programs developed in part by the U.S. telecommunications industry: the Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS).[2] These programs are available to NS/EP authorized users to promote the Nation's security and emergency preparedness functions.

The Government established the existing priority service programs based upon the technologies and interfaces most prevalent at the time they were developed. While past technologies and communications transport mechanisms continue to operate today, the core network transport is universally evolving from circuit-switched to packet-based service technologies. This evolution has helped provide a common operating interface between various access technologies, applications, and providers, including the public switched telephone network (PSTN), private managed networks, and the public Internet.

The Federal Government has begun to prepare for this evolution and to comprehend how the shift to Internet communications and packet-based networks will affect the delivery of NS/EP traffic. Past NSTAC efforts and the ongoing work of the Department of Homeland Security's (DHS) National Communications System (NCS) have analyzed the need for the NS/EP community to keep pace with technology advancements.[3]

1.2 Charge

During the President's 2007 NSTAC Meeting, the Assistant to the President for Homeland Security and Counterterrorism asked the NSTAC to examine concerns regarding the risk, if any, to Internet protocol (IP)-based NS/EP communications traffic, including voice over IP (VoIP), during times of perceived abnormal conditions or network duress. Specifically, the White House requested that the NSTAC determine if network degradation or disruption could affect the receipt or delivery of NS/EP traffic and, if so, provide recommendations to the President regarding measures to ensure the delivery of IP-based NS/EP traffic during those times of network duress.

[2] An overview of the GETS, TSP, and WPS programs can be found at the National Communications System's Web site, http://www.ncs.gov/.

[3] Some of the related NSTAC work efforts include the 2001 *NSTAC Report on Convergent Technologies* and the 2006 *NSTAC Report on Next Generation Networks.* An example of an NCS-led effort is the *2004 NCS Technical Information Bulletin 04-02, Internet Technologies in a Converged Network Environment.*

1.3 Process

The NSTAC examined how service providers transport IP-based traffic across their networks. Several member companies shared information regarding their companies' end-to-end traffic management and routing procedures. They also discussed the solutions their companies use to meet the communications needs of customers. The NSTAC members evaluated strategies and policies guiding how inter-carrier IP-based traffic is transported end-to-end. Furthermore, representatives from Federal agencies briefed the members regarding the evolution of IP-based network infrastructures, the related potential risks, and the standards and technical requirements needed to provide NS/EP authorized users with future IP-based priority services.

Appendix A lists the task force members, industry subject matter experts, and Government participants who contributed to this effort.

2.0 NETWORK EVOLUTION

The global communications architecture is a complex collection of networks, each owned and operated by individual service providers. Technologies are evolving at a rapid pace, increasing the number of options for service providers and customers. The core network is evolving from circuit-switched to IP-based and delivers traffic across the public switched telephone network, private managed networks, and the public Internet. Modern digital technology has allowed the different communications service segments, such as broadcast, cable, satellite, wireless, and wireline, to have common characteristics, such as IP.[4] Service providers have invested billions of dollars to both transform and augment their circuit-switched networks to incorporate the use of IP-based technologies. This investment enables an increasing number of users to exchange an increasing volume of information via both wireless and wireline devices.

Network transport technology is universally standardizing upon IP, a network-layer protocol that contains addressing information and some control information to enable packet routing in networks. IP-based networks, through their flexible, packet-based architecture, inherently can perform many basic functions that a switched or provisioned circuit network cannot do, such as provide more efficient use of bandwidth since it is not a connections-based architecture and simultaneously exchange data to/from remote entities. These fundamental capabilities provide the opportunity to expand the use of networking. The transport layer encompasses the physical and link layers of the IP protocol model. Appendix C discusses some of the major technologies associated with the transport layer.

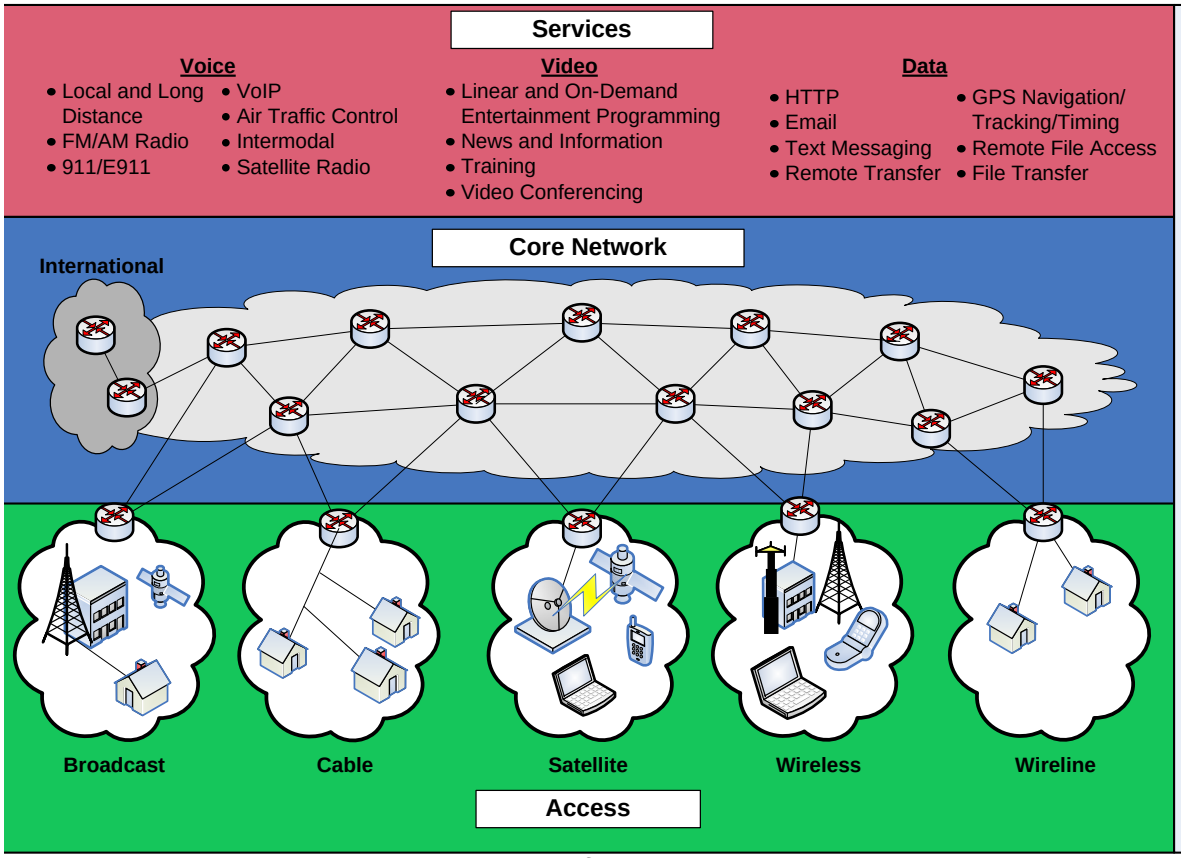
Service providers continue to implement innovative access, switching, and transport technologies, as well as customer premise equipment along with integrating enhanced multiplexing and packet protocols. Carriers also employ technologies that provide the quality of service to which users have become accustomed. These new technologies and architectures must also work with legacy systems and equipment. It is inevitable that telecommunications networks will continue to evolve as new technologies are developed and advanced network elements are incorporated. It is critical that the network continue to perform in the time of a national emergency just as it is essential for service providers to ensure that network improvements keep pace with user demands to exchange information.

Additionally, NS/EP authorized users must be aware of the advancements in telecommunications networks as communications needs evolve and expand. Many service providers offer their customers IP-enabled, application-aware, managed services to deliver security, flexibility, and performance levels for their intranet solutions on a global basis. In addition, to avoid single points of service failures, it is important that NS/EP authorized users discuss their needs for highly reliable access connections with their service provider. These requirements should include diverse routing paths, as well as diverse technologies to access the network where available.[5] The diagram below depicts the diverse services and technologies that service providers offer over the networks.

[4] Additional information on the evolution of the access and core networks is contained in Appendix B.

[5] *NSTAC Financial Services Task Force Report*, April 2004.

Figure 1



Communications Sector Architecture Model [6]

[6] Communications – Sector Coordinating Council's National Security Risk Assessment, May 2008.

3.0 NETWORK MANAGEMENT

Network management is a key requirement to optimize successful operations in both the circuit-switched and packet-switched network environments. Network management techniques evolve as network technology advances, including the ability to manage traffic within and across IP-based network overlays. While managing networks, providers monitor traffic flow and performance to optimize data flow across the network for all users. Network management for IP networks includes monitoring the network for service failures and down ports; service degradation, including packet delay / loss and jitter; traffic anomalies, such as border gateway protocol routing anomalies; and congestion conditions. For circuit-switched voice communications, network management involves responding to incidents such as blocked voice calls during an unusual mass calling event or congestion caused by reduced capacity due to out-of-service conditions, such as trunk connectivity.[7]

In order to optimize network traffic flow, carriers have developed several processes to manage network voice traffic. These processes, based upon network management principles, include:

- Utilizing all available resources;
- Continuous monitoring of traffic volumes and facility utilization;
- Giving priority to connections that make the most efficient use of network resources, in the case of overload; and
- Inhibiting traffic congestion and preventing its spread.

It is critical for telecommunications service providers to be able to manage NS/EP traffic at the time of a national emergency or other event. The growth of high-bandwidth applications has led to higher traffic levels that could affect NS/EP communications traffic. Service providers have historically managed traffic volumes and characteristics in order to provide good performance to customers, including the Government. As newer network technologies call for modified management techniques, effective traffic management will require service providers to continuously monitor networks and traffic flow and take necessary steps to ensure the minimization of network congestion on a day-to-day basis and/or during a national emergency. Enhanced services for NS/EP users in a packet-based network environment must begin with traffic management within the customer equipment, such as enterprise routers, servers, and terminal devices, prior to connecting to the service provider/transport portion of the network.

3.1 IP Routing

The public Internet is comprised of a worldwide commercial collaboration of tens of thousands of individual networks managed by unaffiliated service provider networks using IP to facilitate user-to-user communications. The public Internet uses a structured addressing system through an IP address registry service, that has a standardized language or protocol for communicating between networks; and adheres to a wide array of other technical agreements, such as the ability to translate alphanumeric domain names (for example, www.dhs.gov) into IP addresses through

[7] Additional information regarding network management is contained in Appendix C.

domain registry services and a hierarchical Domain Name System (DNS) infrastructure. This voluntary collaboration permits any individual device connected to the public Internet to interact with another connected device or application anywhere in the world.[8]

Internet service providers (ISP) provide the means to connect a physical location to the public Internet as well as provide the ability to connect to other networks participating in the public Internet. In order for its customers' traffic to reach other ISPs' networks, the ISP must establish a business relationship with one or more other network service providers. Such arrangements, called transit and peering agreements, allow one network to hand off traffic destined for another network. Transport networks are rarely universal and data must therefore use a series of networks to get from its origination point to the end destination. Transit service enables small networks to reach the Internet via larger backbone networks.

Peering traffic between the largest networks occurs via signed peering agreements. The individual policies set by each ISP establish the framework for peering agreements, typically based on a relationship of mutual benefit. Peering agreements provide benefits to both ISPs and give them greater control over the routing of their traffic, as the agreements reduce the costs of transporting traffic between networks and help traffic flow more efficiently. Many of these peering connections occur within commercial carrier-neutral third party exchange points, also called carrier hotels. Within these sites, ISPs and others may choose to interconnect and transmit traffic in instances when a policy agreement is not in place.

Since thousands of unaffiliated networks may deliver IP packets across the Internet, attempts to provide consistent quality of service (QoS) treatment would require network providers to coordinate service offerings, network design and engineering, and operational practices.[9] Such agreements generally do not exist today. QoS is a method for network operators to manage traffic, group together the packets generated by different applications with similar performance requirements, and treat the grouping as a family, or flow class, within a network. The public Internet IP routers make no distinction in how packets are processed, meaning that all packets will receive the same QoS. As such, the public Internet handles packets on a best-effort basis, meaning it cannot provide a guarantee regarding loss rate, bandwidth, delay, and/or jitter.[10]

3.2 Congestion

IP networks transmit data in IP packets. Each IP packet includes both a header that specifies source, destination, and other information about the traffic and the message data itself. Network congestion in the IP network environment occurs when the amount of traffic carried by a link or node exceeds its capacity and results in a deteriorated quality of service level, such as packet

[8] As this report was being developed, attack methods for a significant DNS vulnerability were widely publicized. Other NSTAC work will address security issues such as these.

[9] Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including frame relay, asynchronous transfer mode (ATM), Ethernet and 802.1x networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

[10] Jitter is described as any disruption in packet transmission or delivery.

delay or loss.[11] With non-delay sensitive applications, such as e-mail or instant messaging, the effects of packet delay or loss on the IP network are likely unnoticed by the end user.[12] For delay-sensitive applications, such as VoIP, real-time gaming, or IP television, packet delay or loss can affect the application's ability to operate or its service quality. Service providers, however, have the ability to design and manage their networks to avoid or minimize network congestion and to prevent and respond to network events.

The user will experience network performance that is only as good as the service provider's slowest link. Congestion can occur in many places along a user's communications path. A congested edge, enterprise, or customer premise router can reduce bandwidth and lead to packet loss. Congestion can also occur in a network node, such as a router or switch, from traffic aggregation in which traffic from multiple input ports is destined for a single output port. Network nodes buffer and place traffic exceeding the line speed of the output port in a queue. Waiting in the queue will add delay to the traffic and overfilling the queue will lead to packet loss and degraded application performance. A router placed at the edge of the network to connect various types of residential, cellular, satellite, or enterprise clients to the core network may experience congestion at peak traffic times or during network events. At such times, it may not be able to attain the optimum data transfer speeds if congestion occurs in a router as packet buffers reach capacity. Congestion in edge routers has the potential to affect adversely the performance of applications that depend on the routers to function effectively. This is also true for the edge router at the receiving end. When routers receive more inquires than they have the ability to handle, the user may experience a delayed response. Service providers strive to manage capacity on edge router resources so that users do not experience congestion where their traffic enters the network. Appendix D provides examples of where congestion may occur across the network.

In order to help reduce the effects of network congestion on delay-sensitive applications, a customer can place a fully managed QoS router in its premise. The QoS router employs a robust set of mechanisms to identify voice traffic (inbound or outbound) and ensure that the required amount of bandwidth is available. Additionally, a simple, highly reliable approach to reduce the possibility of network congestion is for service providers to provision a dedicated connection from the customer premises to the IP network edge with bandwidth sufficient to preclude any potential congestion.

[11] Use of the term "congestion" should not be construed to mean a stoppage of data flow; rather it is a delay in the delivery of packets until sufficient network capacity is available to carry them to a device or application.

[12] With these types of services, data can be sent on a "store and forward" basis, meaning that the data is sent when the transmission path is available. Since the action is not real time, the receiver is unaware of the delay.

4.0 APPLICATIONS

As networks have evolved, so too have the supporting operations support systems, software programs, and databases, which have become crucial in their support of the ability to exchange information. The Government, corporations, and consumers rely on systems and supporting databases for a myriad of uses. As applications continue to grow, so does the demand those applications place on the network. Every application (e-mail, instant messaging, data and file sharing, streaming video, VoIP, etc.) uses capacity on the network to exchange information. Time sensitive applications, like voice and video, place additional performance requirements on the network such as limits on propagation, delay, jitter, and packet loss.

VoIP is one example of an application that uses IP packet-based technologies. When a customer uses a VoIP-equipped device, the device converts the call into a digital format, dividing the message into individual IP packets for transmission, and transmits the IP packets across a public or private network. Currently, the majority of callers utilize circuit-switched based technology; because of this, VoIP calls frequently must also traverse circuit-switched networks to connect to users who do not use VoIP-equipped devices and therefore remain on the circuit-switched network. However, as the number of business and residential IP telephony subscribers increase, end-to-end IP calls will also increase in number. In the interim, IP providers are interconnected through circuit-switched providers via peering arrangements.

VoIP services today are typically provisioned either via best-effort routing over the public Internet or via managed services. With the first service, the provider uses the Internet to route the calls to an external voice telephone switch, normally hosted at a traditional central office or similar facility. With this approach, there is a potential single point of failure where the organization's router interfaces with the upstream ISP.

Using managed services, an internal IP private branch exchange (PBX) handles telephone calls on the enterprise local area network (LAN), bringing them out of the organization via a traditional PBX or other voice switch. The advantage to this approach is that there are now two possible paths for a phone call, a primary path through the PSTN and a secondary path through the Internet as is done in the first option above.

In both cases, the VoIP phones use the same LAN infrastructure as the desktop workstations, thus saving on the cost of having a second parallel-wired telephone infrastructure. Some VoIP products use only the public Internet to route voice calls, and depend on end-to-end routing of VoIP packets. Other products have a voice switch or gateway inside the customer's premise that takes the VoIP packets off the LAN and connects them to the PSTN as though they were traditional analog or digital voice calls. NS/EP authorized users should carefully consider the reliability, security, and performance of best efforts routing across the public Internet as a transport path versus the use of traditional PSTN or managed networks as a transport path. Additionally, NS/EP authorized users should consider using managed services as detailed in the section below.

5.0 MANAGED SERVICES

Carriers and service providers typically offer managed services as an integrated, "packaged" solution to meet the requirements of enterprise customers. This can include communications and network services with integrated provisioning and operations management, application hosting and management services, data processing and storage services, mobility solutions, business continuity solutions, or combinations thereof. These offerings frequently include "private" communications capabilities through means such as dedicated circuit paths, software defined networks, and virtual private networks (VPN). Managed services are private communications because they provide only connections between certain points that the customer authorizes or is dedicated to delivering a particular type of capability. Managed communications services address the need for communications' security, separation, and resilience at significantly lower cost than construction of a unique, dedicated network.

With a high degree of collaboration with its customer, a service provider can keep mission-critical data networks carrying both voice and data traffic running successfully during network anomalies or instances of congestion. Managed services are reliable, secure, and cost-effective solutions that take advantage of converged infrastructure.

Within a single network, a service provider can offer performance/reliability assurances because it is able to monitor and manage services on an end-to-end basis. When the customer first contracts services, the customer and service provider can devise a contractual service level agreement (SLA) to define the QoS flow classes and the performance within a specified range of parameters, including availability, latency, jitter, and packet loss. The customer and service provider define how to recognize the packets generated by the customer's various applications and specify the mapping of each to a flow class. The parties also reach agreement regarding what will occur if the customer generates more than the agreed-upon volume of flow for a particular class.

In some cases, a customer enters into multiple agreements with individual service providers to receive a specific quality of service within and among service providers.[13] In this instance, the carriers engineer and manage the service to meet the customer's requested QoS for performance and reliability assurances. The customer has the responsibility to mark the traffic per the agreement with each service provider in order for the service provider to recognize the markings and route the traffic accordingly.

A VPN generally takes full advantage of the QoS differentiation options within the service provider's network. It can also use end-point encryption and/or logic in the service provider's network routers to permit traffic to move only between the points authorized by the customer. In this way, the service provider's managed service capabilities delivers performance tailored to the customer's business applications while providing the security business customers seek when using a private network. Furthermore, the use of a common physical infrastructure reduces costs.

[13] Carriers are working to provide a service within a public network environment where QoS and priority markings are recognized and acted upon throughout the entire network.

Although much of a VPN's traffic may be on one service provider's network, it is possible to enable connections to locations on different service providers' networks, though such connections will typically require encryption to ensure that they are secure. For example, remote access working arrangements may use inter-carrier connections. Because these connections can traverse the public Internet, which involves crossing multiple unaffiliated physical networks, they will not have service assurances. Likewise, it is possible for a VPN to have connections to the public Internet. A public Internet connection, however, would need the protection of firewalls and other security technologies, and the end-to-end connection would not be subject to service assurance.

The Federal Government uses managed services to meet its communications needs.[14] The use of managed services could be expanded to provision NS/EP services within the new IP-based environment.

[14] GSA's Networx Universal and the National Capital Region's Washington Interagency Telecommunications System contracts provide enhanced communications services and are examples of Government's use of managed services.

6.0 GOVERNMENT AND INDUSTRY COLLABORATION

The U.S. Government has long recognized the Nation's increasing reliance on telecommunications services. During times of emergency, crisis, or war, personnel with NS/EP missions must have confidence that they will not lose their access to the priority-enabled services supported by communications providers' networks. For several decades, the Government and its industry partners have worked to develop the centralized, well-established, and mature set of technical standards and business practices that exist in the PSTN today, supporting a ubiquitous national NS/EP communications capability. The evolving IP-based data networks are highly decentralized and operate in environments where Government and industry have only just begun to address and develop technical specifications and standards.

6.1 Next Generation Network-Based Priority Services

The Nation's PSTN-based NS/EP capabilities continue to support key leadership and first responders, but with an ever-increasing consumer and commercial adoption of IP-based communications, its long-term viability is diminishing. Many agencies and organizations have therefore undertaken next generation network (NGN) NS/EP planning efforts to replace this resource.

Within the public Internet, a best effort treatment of packets cannot guarantee that NS/EP traffic receives end-to-end priority service; therefore, the NCS and its industry partners have examined ways to optimize priority using an "industry requirements" model, with inputs from consultants, equipment vendors, and service providers.[15] This model was previously successful when developing the GETS and WPS solutions. In December 2007, the NCS completed the first of several phases of standards work, laying the foundation for industry to plan for NS/EP service development (in other words, voice, then video and data) within the industry's IP multimedia subsystem architecture. The report, titled *National Security and Emergency Preparedness Internet Protocol Multimedia Subsystem Core Network Industry Requirements for Next Generation Networks Government Emergency Telecommunications Service, Phase 1, Voice Service* includes an analysis of potential call connection combinations and various evolving network architectures. It is important that Congress fund the NCS work in this area to continue industry and Government collaboration and to ensure that advanced NS/EP services are operational when needed.

6.2 Industry Standards

Several global standards bodies are addressing NS/EP next generation IP-based priority services delivery. Standards bodies developing provisions for special handling of priority services to support critical communications in the emerging IP packet-based network environment include:

- The Internet Engineering Task Force

[15] It is also important to note that end-to-end delivery requires the customer to be able to receive the traffic that is delivered to them.

- International Telecommunication Union - Telecommunication Standardization Sector
- Alliance for Telecommunications Industry Solutions
- The European Telecommunications Standards Institute's Telecoms and Internet Converged Services and Protocols for Advanced Networks
- Third Generation Partnership Project

Many countries, including the United States, participate in these bodies to formulate standards for future worldwide adoption. At a time when countries such as China, Japan, and South Korea are becoming more actively engaged in the standard-setting process, it is important that the United States commit appropriate resources to maintain a leadership position. This will help ensure the United States has the opportunity to influence the global adoption and implementation of standards that will drive the long-term effects on IP-based prioritization.

7.0 LEGAL AND REGULATORY POLICIES

Directed by Presidential Executive Order,[16] the NCS is responsible for ensuring "that a national telecommunications infrastructure is developed which is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies other entities, including telecommunications in support of national security leadership and continuity of government."[17]
In fulfillment of its responsibilities, the NCS manages the TSP and GETS programs, both NS/EP priority services that provide nationwide, ubiquitous voice and voice-band data service in the PSTN. Since 2001, NCS also has managed the WPS, which provides priority NS/EP service in the cellular wireless portion of the PSTN.

In 2000, the Federal Communications Commission (FCC) issued an order establishing that the priority services offered to NS/EP authorized users were *prima facie* lawful under the *Communications Act of 1934* as amended, and not an unreasonable preference or discrimination in contravention of Section 202(a) of the Act.[18] These priority services support critical functions such as national security leadership, continuity of government, public health, and safety, maintenance of law and order, and disaster recovery during national security emergencies.

The authority contained in this FCC precedent must be maintained to ensure networks are capable of providing priority communications for NS/EP authorized users in the future. As explained in this paper, packet-switched-based technology infrastructure carrying higher bandwidth applications continue to replace the PSTN and other legacy circuit-switched networks. As that IP technology becomes more widespread and plays an increasingly important role in supporting NS/EP services, those services—and the network management techniques that make them possible—must be permitted to evolve in an IP-based environment. For that evolution to occur, the proper legal and regulatory policies must be in place to ensure NS/EP traffic continues to have priority treatment on IP-based networks. Consistent with its ruling that priority access services offered by carriers to NS/EP authorized users are "*prima facie* lawful" under the Communications Act and do not constitute "unreasonable discrimination" under section 202 of the Act,[19] the FCC should specifically confirm that the same is true with regard to IP-based priority access services offered by IP-based providers to NS/EP users.[20]

---

[16] In 2007, in the President's National Continuity Policy (NCP), the Secretary of Defense was tasked in coordination with the Secretary of Homeland Security to provide secure, integrated, continuity of Government communications to the President, the Vice President, and certain key executive departments and agencies. In addition, the NCP directed the heads of the executive Departments and Agencies to "plan, program, and budget" for those continuity capabilities. See National Security Presidential Directive 51/ Homeland Security Presidential Directive 20.

[17] Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (amended by E.O. 13286 of February 28, 2003).

[18] FCC's Second Report and Order - Establishment of Rules and Requirements for Priority Access Service, WT Docket No. 96-86, Adopted July 3, 2000.

[19] Id.

[20] The FCC previously sought comment regarding services and applications making use of IP and the the impact that IP-enabled services have had and will continue to have on the United States' communications landscape. See Notice of Proposed Rulemaking on IP-Enabled Services, WC Docket No. 04-36. DHS filed Comments in response to the NPRM noting that "[a]ll VoIP providers, ISPs and IP transmission carriers should be permitted to

8.0 KEY FINDINGS

The NSTAC finds the following:

- The core networks are universally evolving from circuit-switched to packet-based service technologies. The network management principles employed by the carriers evolve as the technology of the networks advances, including the ability to manage traffic within and across IP-based network overlays.

- The growth of high-bandwidth applications has led to higher traffic levels and could affect NS/EP communications traffic. Service providers design and manage their networks to avoid or minimize network congestion and to prevent and respond to network events.

- Enhanced services for NS/EP authorized users in a packet-based network environment must begin with traffic management within the customer equipment, such as enterprise routers, servers, and terminal devices, prior to connecting to the service provider/transport portion of the network.

- The public Internet handles packet routing on a best-effort basis, meaning it will try its best to forward user traffic, but can provide no guarantees regarding loss rate, bandwidth, delay, and/or jitter.

- Within a single network via a managed service offering, a service provider can offer performance/reliability assurances because it is able to monitor and manage services on an end-to-end basis. A customer can also enter into an agreement with multiple service providers to receive a specific QoS from the service providers for a managed service.

- The Federal Government uses managed services to meet its communications needs. NS/EP services could also be provisioned using managed services within the new IP-based environment.

- The Nation's PSTN-based NS/EP capabilities continue to support key leadership and first responders using GETS, WPS and TSP, but with the increasing consumer and commercial adoption of IP-based communications, its long-term viability is diminishing.

- The NCS is working with industry partners to establish IP-based priority services using an "industry requirements" model, which was previously successful in developing the GETS and WPS solutions. Continued funding for these NCS activities is essential to

provide assured service enhancements (including priority treatment) to NS/EP marked traffic while not providing such enhancements to other traffic." In its comments, DOD also stated that "NS/EP considerations provide a compelling rationale for applying a certain amount of regulation to IP-enabled services. The purpose of such regulation would be to ensure the prioritized availability of certain communication services in times of emergency or national crisis."

enable continued Government and industry collaboration and to ensure that advanced NS/EP services are there when needed.

- Global standards bodies are addressing NS/EP IP-based priority services delivery. The United States has an opportunity to influence the outcomes of these standards bodies by actively participating and leading the standards development process.
- The FCC found that the provision of priority services offered to NS/EP authorized users was *prima facie* lawful under the *Communications Act of 1934*. These priority services support critical functions such as national security leadership, continuity of government, public health, and safety, maintenance of law and order, and disaster recovery during national security emergencies. This provision must maintain the authority to ensure that networks remain capable of providing priority communications for NS/EP authorized users in the future.

9.0 RECOMMENDATIONS

The NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, that the President should:

- In the short term, establish a policy that requires Federal departments and agencies to:
  - Ensure their enterprise networks are properly designed and engineered to handle high traffic volume;
  - Manage traffic through QoS programming in its routers to prioritize traffic, including NS/EP traffic; and
  - Expand the use of managed service agreements to provision NS/EP services within the new IP-based environment.

- In the long term, require Federal departments and agencies to remain actively involved in standards development of priority services on IP-based networks by supporting efforts to:
  - Provide adequate funding that will be used to develop timely solutions across all technology platforms; and
  - Commit appropriate resources to actively participate in and lead the global standards bodies' efforts to address NS/EP IP-based priority services.

- Petition the FCC for a declaratory ruling to confirm that network service providers may lawfully offer IP-based priority access services to NS/EP authorized users.

APPENDIX A

PARTICIPANT LIST:
TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER WORKING GROUP PARTICIPANTS

APPENDIX A

PARTICIPANT LIST: TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER WORKING GROUP PARTICIPANTS

TASK FORCE MEMBERS

AT&T, Inc.	Mr. Thomas Hughes
	Ms. Rosemary Leffler
Bank of America Corporation	Mr. Roger Callahan
The Boeing Company	Mr. Robert Steele
CSC	Mr. Guy Copeland
Juniper Networks, Inc.	Mr. Robert Dix
Microsoft Corporation	Ms. Cheri McGuire
Nortel Networks	Dr. Jack Edwards
Qwest Communications International, Inc.	Ms. Kathryn Condello
Raytheon Company	Mr. William Russ
Science Applications International Corporation, Inc.	Mr. Henry Kluepfel
Sprint Nextel Corporation	Ms. Allison Growney
Telcordia Corporation	Ms. Louise Tucker
Verizon Communications, Inc.	Mr. James Bean

OTHER PARTICIPANTS

AT&T, Inc.	Dr. Bobbi Bailey
Bank of America Corporation	Mr. Larry Schaeffer
CSC	Ms. Janet Gunn
European Commission	Mr. Detlef Eckert
	Ms. Anna Snow
George Washington University	Dr. Jack Oslund
Juniper Networks	Mr. Tom Van Meiter
Qwest Communications International, Inc	Ms. Kathryn Condello
	Mr. R. David Mahon
	Mr. Thomas Snee

Renesys Corporation	Dr. Earl Zmijewski
Sprint Nextel Corporation	Mr. John Stogoski
VeriSign, Inc.	Mr. William Gravell
Verizon Communications, Inc.	Mr. Marcus Sachs

GOVERNMENT PARTICIPANTS

Department of Defense	Mr. Anthony Bargar
	Ms. Catherine Creese
	Mr. Marna Harris
	Mr. Herb Herrmman
	Capt. John Kennedy
	Mr. Mark Lauver
	Ms. Hillary Morgan
	Mr. Dan Wenk
Department of Homeland Security	Ms. Sue Daage
	Mr. Vern Mosley
	Mr. An Nyguen
	Mr. Frank Suraci
	Mr. Will Williams
Executive Office of the President	Mr. Billy O'Brien
Federal Communications Commission	Mr. Richard Hovey
Federal Reserve Board	Mr. Wayne Pacine

APPENDIX B

ACCESS AND CORE NETWORKS

APPENDIX B
Access and Core Networks

Access describes the part of a communications network that subscribers use to connect to their immediate service provider. It refers specifically to the series of physical connection methods that interconnect a consumer/business termination point and its service provider, such as the local exchange carrier, Internet service provider (ISP), or cable television service provider.[1] Access networks are evolving to include fiber optic technology as providers bring the benefits of high capacity and value-added services over broadband networks to customers. To avoid single points of service failures, it is important that national security and emergency preparedness (NS/EP) authorized users discuss their needs for highly reliable access connections with their service provider. These requirements should include diverse routing paths, as well as diverse technologies to access the network where available.

A core network transports a high volume of aggregated traffic over significant distances via fiber optic cable, microwave radio, copper cable, or satellite and interconnects access networks across the country. Core networks span the globe mainly using submarine fiber optic communications cable systems as well as land-based fiber cable networks.

These core networks interconnect at numerous points throughout the Nation, forming the communications infrastructure. Core networks are today primarily composed of terrestrial and undersea wireline networks, with satellite links being an exception.[2] The same core network delivers traffic for the public switched network, private managed networks, and the public Internet.[3] The voice core networks are evolving from circuit switched to packet-based. Service providers deploy self-healing technologies to protect their physical networks, as well as leverage the interconnection of these networks to provide resilience and redundancy to sustain availability during an incident. As discussed in the *NSTAC Report to the President on Network Operations Centers*, service providers operate network operations centers to configure, monitor, and provision the core network nodes.[4] Service providers collect various forms of information about their networks, including statistics, alarms, and utilization data, which are important tools that service providers use to monitor network health and performance and re-route traffic in the event of congestion.

Interconnection agreements or tariff filings outline how to handle the exchange of voice traffic between service providers across the public switched telephone network (PSTN). To meet these obligations, service providers enter into interconnection agreements or file tariffs, which include

[1] The local telephone exchange contains automated switching equipment that directs a call or connection to a consumer.

[2] The satellite segment can provide worldwide transport services as well, however the access segments presented within the architecture generally use wireline core networks for sending traffic (though cable and broadcast may receive substantial video feeds via satellite). As a result, core networks generally refer to the wireline core network and specific mention is made of the satellite segment's role as a core network.

[3] The public Internet is an application that is delivered over networks and not a network itself.

[4] *NSTAC Report to the President on Network Operations Centers.* February 2008.

the transmission and routing of telephone exchange service and exchange access at any technically feasible point within the provider's network. Additionally, service providers are required to establish reciprocal compensation arrangements for the transport and termination of telecommunications. The terms and conditions contained in interconnection agreements outline how providers deliver traffic and compensate one another for the use of their networks. These terms and conditions also outline the steps for dispute resolution should any issue arise.

ISPs interconnect through dedicated connections or at peering points, and establish agreements to exchange or transit traffic. In addition, smaller ISPs may elect to purchase access services from larger, or Tier 1, backbone providers. These interconnections only provide for exchange of "public" Internet traffic. Internet peering generally does not include interconnection of private (for example, enterprise) or carrier core network traffic or services that include advanced features.

APPENDIX C

TRANSPORT LAYER

APPENDIX C
TRANSPORT LAYER

Multi-Protocol Label Switching

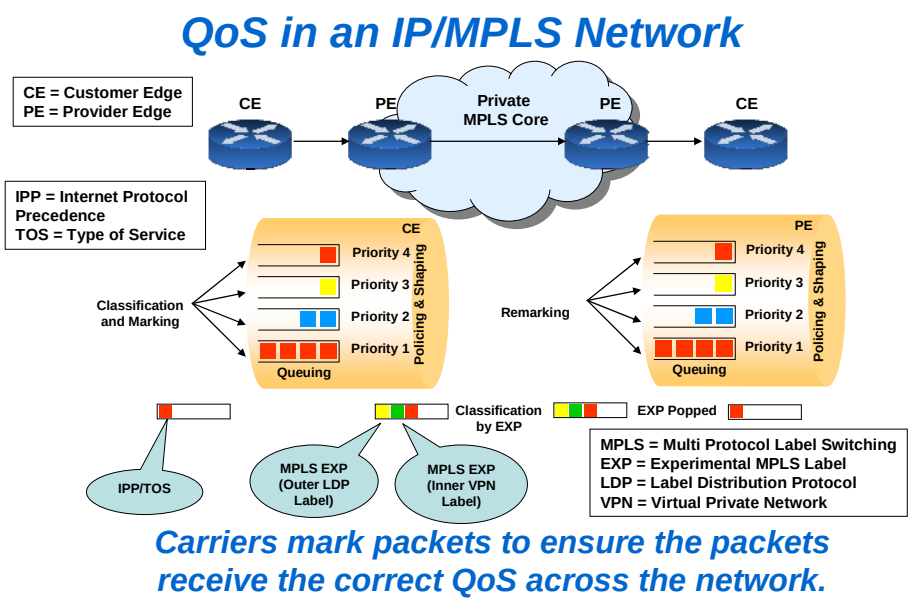
Many service providers make use of the Multi-Protocol Label Switching (MPLS) technology layer in their network infrastructure to provide capabilities and service features beyond that of Internet protocol (IP) alone, such as complex network traffic engineering and sharing same network infrastructure amongst Internet access services and secured virtual private network (VPN) services. Use of this technology enables carriers to achieve economy-of-scale and lower unit cost. IP routing protocols have no awareness of the capabilities and characteristics of the underlying physical network. MPLS addresses this limitation by enabling the handling of IP packets based on mapping the packets to a flow class. These flow classes can utilize predetermined edge-to-edge paths that have predictable performance characteristics, as compared to the hop-by-hop, best available route handling inherent with public Internet routing. Packet mapping occurs each time a customer's IP-based router sends traffic into the MPLS network.

At the entry point to the MPLS network, the network encases the IP packet in a new envelope called a label and directs it to the far side of the MPLS network, based on the edge MPLS router associated with the destination IP address. The logic for routing across the available bandwidth is a function of the flow class of the MPLS packet. At the far edge, the MPLS removes the envelope, revealing the original IP information. A service provider that employs MPLS and supports the public Internet usually uses a single flow class for all traffic directed to or coming from the public Internet. This flow class will not have any assured level of performance. This is consistent with the treatment of all public Internet traffic.

MPLS enables the service provider to define classes of service, also known as quality of service (QoS), across their networks so that the treatment of customers' traffic is different depending upon the application and its performance requirements. For example, VoIP is a delay-sensitive application and business customers typically choose to give VoIP the best treatment or highest QoS that the carrier offers. Carriers offer service level agreements to managed services customers based on the traffic performance characteristics as defined by each QoS.

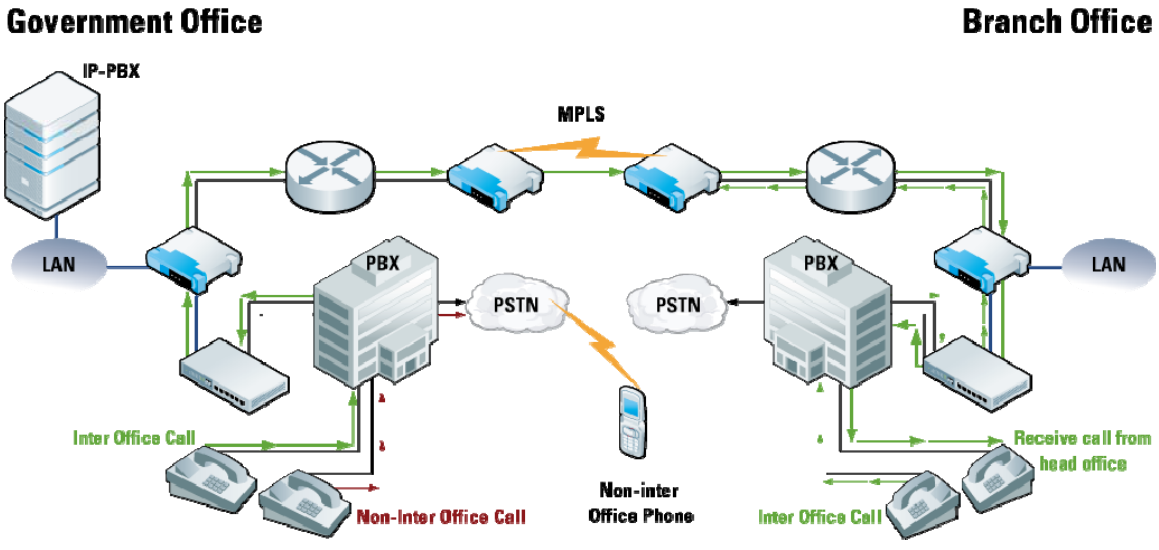
The diagram below illustrates how the assignment of various flow classes using the QoS functionality of MPLS gives IP traffic priority. Carriers mark packets to ensure the packets receive the correct QoS across the network.

Figure 1



The diagram below depicts how a Government agency office with an IP private exchange (PBX) system can connect with one of its branch offices using MPLS to increase the QoS of the communications path.

Figure 2



Service providers can also use MPLS to ensure national security and emergency preparedness (NS/EP) IP traffic receives the appropriate QoS levels as required by the associated applications.

Ethernet

Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). It defines a number of wiring and signaling standards for the physical layer, through means of network access at the media access control (MAC) and data link layer, and a common addressing format. Ethernet is standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN technology. The initial deployment occurred in 1980.

Ethernet is the most-used LAN worldwide. In fact, most data traffic begins or ends on an Ethernet interface. Ethernet allows high bandwidth connectivity, supports multimedia applications, and delivers storage services and server consolidation. The interface speeds on Ethernet have evolved from 10 Mbps to 10 Gbps.

Ethernet technologies allow scalability, traffic engineering, QoS, reliability, and manageability to allow service providers to shape it as an infrastructure for converged, next-generation networks that can better support NS/EP traffic. Ethernet is capable of allowing service providers to deploy native Ethernet services initially, and interwork with MPLS services.

Asynchronous Transfer Mode

Public carriers implement asynchronous transfer mode (ATM) to provide high bandwidth service. ATM is normally deployed in conjunction with a Layer 1 synchronous optical network (SONET) infrastructure. ATM is feature-rich and offers many different services, but other technologies that offer more cost effective capacity and simplified management to integrate voice and video continue to replace ATM. One of the key aspects is its wide support by the American National Standards Institute and International Telecommunication Union for carrying a complete range of user traffic for voice, video, and data for any type of physical media. ATM scalability is limited due to the high cost of chip sets and limited number of implementations that can exceed OC-192 speeds, as IP device requirements are for operation at speeds up to OC-768.

ATM contains QoS capabilities for delivery of real-time traffic and other delay sensitive traffic. QoS is achieved through assignment of traffic to constant bit rate (CBR), variable bit rate, and unspecified bit rate QoS. For example, ATM CBR allows specification of a QoS to achieve controlled latency, jitter and throughput for real-time applications such as voice or video traffic.

The Internet Engineering Task Force has defined a suite of protocols for carrying IP traffic over ATM, and these standards not only address delivery of best effort traffic, but also standardize the use of RSVP to signal IP application requirements to the ATM infrastructure to allocate QoS resources. Since ATM is still deployed at the edges of many networks, ATM CoS will continue to be used as a means to deliver real-time traffic for the near future. However, the emergence of new technologies such as dense wavelength division multiplexing (DWDM), MPLS and Gigabit

Ethernet will more tightly integrate network management and provide higher performance for lower cost than ATM.[1]

Synchronous Optical Networks

Synchronous Optical Networks (SONET) belong to a family of fiber optic transmission rates from 51.84 Mbps (OC-1) to 39.812 Gbps (OC-768) created to provide the flexibility needed to transport many digital signals with different capacities. Moreover, SONET is an optical interface standard that allows inter-working of transmission products from multiple vendors. SONET is widely deployed by carriers, often in a physical ring topology with fast switching between segments or sections (50 milliseconds), with multiple fibers providing transport redundancy. SONET has been widely implemented within carrier domains and has only recently been challenged by DWDM, which, although it lacks robust network management standards, offers higher aggregate speeds and is far less expensive. SONET traditionally has been used to carry time domain multiplexing (TDM) traffic, which is considered not practical for IP traffic due to its high cost; other criticisms of SONET include bandwidth limitations, high overhead and high costs of provisioning. The strongest argument for its continued use in the transport network arena is its strong network management capabilities, a strong set of standards, and the large embedded base of equipment used in carriers' networks.

SONET, in spite of its limitations, has a key role in the next generation telecommunications infrastructure. Carriers have considerable investment in their SONET networks and cannot see enough revenues coming from new services to justify building overlay networks. As a result, SONET will likely not be replaced by an all-optic network or by a native Ethernet transport network within the next ten years. SONET equipment manufactures are evolving their equipment offerings to conform to the carriers' requirements demanding affordable, standards-based platforms that are highly scalable and deliver packet and TDM services both seamlessly and without manual configuration. To achieve these goals, vendors are developing their products to span from the customer core, using advances in multi-protocol traffic adaptation, and developing their products for end-to-end operations management. Industry experts predict that multi-service SONET platforms will be as fundamental to telecommunications networks in the coming decade as routers were to the Internet during the 1990s.[2]

[1] See section 2.1.3 of the *NCS Technical Information Bulletin 04-2: Internet Technologies in a Converged Network Environment*; dated December 2004.

[2] See section 2.1.4 of the *NCS Technical Information Bulletin 04-2: Internet Technologies in a Converged Network Environment*; dated December 2004.

APPENDIX D

CONGESTION

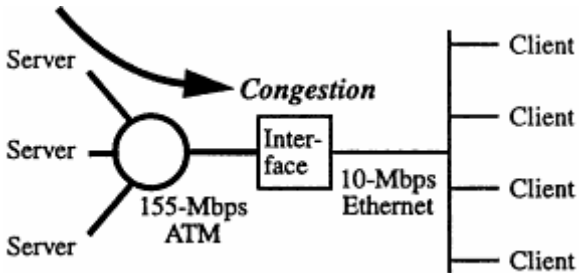
APPENDIX D : CONGESTION

A stream of data is separated into packets for transit across an Internet protocol (IP) network. Each IP packet includes both a header that specifies source, destination, and other information about the traffic and the message data itself. Network congestion in the IP network environment occurs when the amount of traffic carried by a link or node exceeds its capacity and results in a deteriorated quality of service level, such as packet delay or loss. [1] With delay insensitive applications, such as e-mail or instant messaging, the effects of packet delay or loss in the IP network will likely go unnoticed by the end user.[2] For delay sensitive applications, such as Voice over Internet Protocol (VoIP), real-time gaming, or IP television, packet delay or loss can affect the application's ability to operate or its quality of the service. Service providers design and manage their networks to avoid or minimize network congestion and to be able to prevent and respond to network events.

The user will only experience performance as good as the slowest link. Congestion can occur in many places along a user's communications path. One cause of congestion can be a mismatch in speed between networks. For example, national security and emergency preparedness (NS/EP) authorized users on a low-speed local area network (LAN) connection, such as a 10 Mbps Ethernet, connecting to servers on high-speed networks, such as a 155 Mpbs asynchronous transfer mode (ATM) over OC-3, may experience congestion at the interface between the networks as the diagram below illustrates. Additionally, if a 10 Mbps connection is supporting hundreds of users within an office, congestion could occur as the users send/receive data due to the size of the connection.

Figure 1

Congestion Due to Speed Mismatch



Congestion can also occur in a network node, such as a router or switch, from traffic aggregation in which traffic from multiple input ports is destined for a single output port. Traffic exceeding

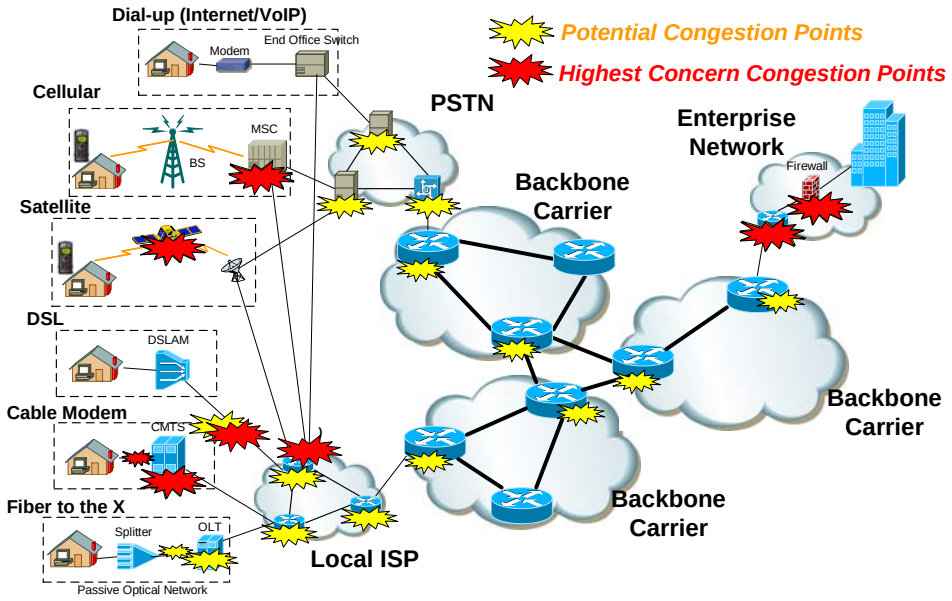
[1] Use of the term congestion should not be construed to mean a stoppage of data flow; rather it is a delay in the delivery of packets until sufficient network capacity is available to carry them to a device or application.

[2] With these types of services, data can be sent on a store and forward basis, meaning that the data is sent when the transmission path is available. Since the action is not real time, the receiver is unaware of the delay.

the line speed of the output port will be buffered and placed in a queue. Waiting in the queue will add delay to the traffic and overfilling the queue will lead to packet loss and degraded application performance. A congested edge, enterprise, or customer premise router can reduce bandwidth and lead to packet loss. A router placed at the edge of the network to connect various types of users, such as residential, cellular users, satellite communications, or enterprise clients, to the core network may experience congestion at peak traffic times or during network events. At such times, it may not be able to attain the optimum data transfer speeds if a router is congested as packet buffers reach capacity. Congestion in edge routers has the potential to adversely affect the performance of applications that depend on the routers to function effectively. This is also true for the edge router at the receiving end. If a router is receiving, more inquires than it is designed to handle, the users may experience a delayed response. Service providers generally strive to manage capacity on edge router resources so that users do not experience congestion where their traffic enters the network.

Figure 2

Diagram of Potential Congestion Points



Congestion for digital subscriber line or dial-up customers is generally not at the digital subscriber loop access multiplexer (DSLAM); rather, it is the transport from the Internet service provider (ISP) point of presence to the DSLAM. An inadequate number of ports on the network access server at the ISP can lead to congestion. Further, an overloaded web server could experience congestion during a period of high use. In addition, a user may overload their personal computer with multiple tasks, thus leading to slower service and an ineffectiveness use of an application.

In order to help reduce the possibility of network congestion, a customer can place a fully managed quality of service (QoS) router on its premise. As described in section three, the QoS router has a robust set of QoS mechanisms it can employ to identify voice traffic (inbound or outbound) and ensure that the required amount of bandwidth is made available. Additionally, a highly reliable and simple to implement approach to reduce the possibility of network congestion is to provision a dedicated connection from the customer premises to the IP network edge with bandwidth sufficient to preclude any potential congestion.

APPENDIX E

NETWORK MANAGEMENT

APPENDIX E:
NETWORK MANAGEMENT

Network management is a key requirement for successful operations in both the circuit switched and packet switched network environment. Network management techniques evolve as network technology advances, including the ability to manage traffic within and across Internet protocol-(IP) based network overlays. While managing networks, providers monitor traffic flow and performance to optimize data flow across the network for all users. Network management for IP networks includes monitoring the network for service failures or down ports; service degradation including packet delay/loss and jitter; traffic anomalies, such as border gateway protocol routing; and congestion conditions. For circuit-switched voice communications, network management involves responding to incidents such as during an unusual mass calling event or congestion caused by reduced capacity due to out-of-service conditions, such as trunk failure.

To control the traffic, network managers generally have two categories of mechanisms:

- **Expansive controls** temporarily expand the available capacity and successfully complete customer service via alternate paths. A simple example is moving service onto a preprovisioned protection path, which exists in the network solely for the purpose of service protection in the event of the loss of a primary path. More complex examples involve rerouting circuit switched voice calls through alternate routes, or adjusting the flow parameters of IP traffic, to redirect traffic away from a congested path and onto paths that have capacity available to handle the extra load.
- **Protective controls** stop traffic that cause network harm due to volume-related congestion, such as radio call-in promotions when call volumes traditionally increase or during an intentional distributed denial-of-service (DDOS) attack. Filtering and eliminating malicious traffic associated with cyber attacks or canceling traffic to a destination that is known to be out of service so that it does not consume unnecessary capacity are examples of a protective control response.

The terrorist attacks of September 11, 2001, in New York City provided an example of the importance of managing traffic to avoid network congestion. This attacks resulted in increased network traffic as people attempted to locate each other, in some cases between 150 and 400 percent of the normal calling volume, with most of it concentrated toward lower Manhattan. Carriers recognized that the attack had destroyed some business offices and their associated communications equipment. Rather than transporting traffic destined for the impacted area from another location and consuming network capacity, carriers blocked voice traffic at its origination, keeping resources available to transport other traffic with a higher probability of completion. Other examples of network congestion events include holidays that cause a high volume of traffic, mass calling events, bad weather, or cyber attacks.

The three basic key enablers of traffic management on the Internet consist of the IP addressing concept, routing protocols, and the physical infrastructure of routers and connectivity that provides the communications pathway. Specifically:

- IP addressing allows the unique identification of any device connected to the public Internet. The addresses are associated with specific ports on physical networks. Each service provider manages the assignment of one or more continuous ranges of IP address. The structure of the address allows fast identification of the network, or autonomous system, to which any device is currently connected. In effect, the service provider assigns each active device a unique IP address, which is associated with a specific port, or physical termination, within the service provider's network.
- Routing protocols allow one network to exchange information with another network. When a packet is received, the destination address is compared to the information in the routing table. The packet is then passed to the next router, which advances the packet to its ultimate destination at the lowest cost. This means that information moves across an IP network, like the Internet, by hopping from one router to the next with each hop moving it closer to its destination. This allows billions of devices to connect users without the need for each individual network and device to have a predefined path to its destination.
- The ability for two devices to communicate also requires Internet service providers (ISP) to establish a physical connection, which consists of either fiber or copper cables, to buildings and equipment. The ISPs deploy the routers that analyze the IP addresses associated with each packet and invest in the facilities connecting routers to each other and to the end users.

APPENDIX F

TERMS AND ACRONYMS

APPENDIX F:

Terms and Acronyms[1]

ATM	Asynchronous Transfer Mode
CBR	Constant Bit Rate
DHS	Department of Homeland Security
DSLAM	Digital Subscriber Loop Access Multiplexer
DWDM	Dense Wavelength Division Multiplexing
FCC	Federal Communications Commission
GETS	Government Emergency Telecommunications Service
IP	Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN	Local Area Network
MPLS	Multi Protocol Label Switching
NCS	National Communications System
NGN	Next Generation Network
NS/EP	National Security and Emergency Preparedness (NS/EP)
NSTAC	President's National Security Telecommunications Advisory Committee

[1] *Newton's Telecom Dictionary 22nd Edition* used for Terms.

PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SLA	Service Level Agreement
SONET	Synchronous Optical Network
TDM	Time-Division Multiplexing
TSP	Telecommunications Service Priority
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WPS	Wireless Priority Service
X.25	An ITU-T standard network layer protocol